

C15A - Amenazas Informáticas

Introducción a la seguridad informática

Seguridad informática

¿Podemos pensar en una cuarta revolución industrial? Aunque en la historia de la humanidad podemos definir claramente tres revoluciones industriales, lo cierto es que existe una cuarta y, es precisamente, la que estamos viviendo en la actualidad, gracias a la aparición de las tecnologías de información y las comunicaciones (TIC), junto con Internet.

En las últimas dos décadas, las TIC han adquirido un valor en dimensiones que nunca antes había ocurrido en la historia, generando profundas transformaciones en todos los ámbitos socioeconómicos y, por supuesto, de la mano aparecieron conductas ilícitas cometidas sobre los datos, la información, los programas y todo aquel recurso tecnológico susceptible de ser manipulado ilícitamente.

La seguridad informática, o ciberseguridad, es una disciplina que se encarga de proteger la integridad y la privacidad de los datos y toda la información que

se encuentre alojada en un sistema informático. La idea principal es que se pueda evaluar la seguridad de los sistemas de cómputo y redes para, posteriormente, protegerlos de los ataques informáticos que se pueden llevar a cabo a los sistemas.

Pero, ¿esto fue siempre así? A lo largo de la historia, esta seguridad se ha ido transformando, gracias a los controles y auditorías sobre los sistemas, explotando las vulnerabilidades que se puedan encontrar en los mismos. Se han implementado medidas de seguridad física y lógicas en conjunto con la seguridad en Internet.

Por otro lado, sería fantástico poder analizar de forma particular cuál es el impacto que ha causado en la sociedad, en sus normas jurídicas y éticas. Además, reconocer e identificar los delitos informáticos y las consecuencias legales que implican el no acatarlas.

Bien, ha llegado el momento de adentrarnos en el estudio de este maravilloso mundo de seguridad.

Objetivos del módulo

En términos generales esperamos que a lo largo de este módulo podamos:

- Identificar todo tipo de amenazas informáticas, la importancia de los fallos, vulnerabilidades y las contingencias que se pueden tener.
- Conocer los aspectos generales de la seguridad de los sistemas informáticos, criterios generales de medidas de seguridad y protección a tener en cuenta.
- Brindar al futuro profesional conocimientos acerca de la importancia de la informática en la sociedad, los códigos de ética, moral y práctica profesional.

Ciberseguridad y tipos de amenazas

La seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, especialmente, en la información que se transmite a través de las redes de computadoras. Para minimizar todos los riesgos a la infraestructura y a la información se han creado a lo largo de la historia múltiples métodos, como estándares, protocolos, reglas, herramientas y obviamente leyes informáticas.

Debemos tener en cuenta que la seguridad informática únicamente se va a centrar en el medio de comunicación por el cual va a viajar la información. No debemos confundir este término con el de seguridad de la información, ya que esta última puede estar en diferentes medios y no solo en los medios informáticos.

Bajo este último concepto, la seguridad informática va a identificar, eliminar vulnerabilidades y proteger de ataques maliciosos a los equipos de cómputo, servidores, redes informáticas y todo aquel medio informático por el cual se transmita información.

Tipos de amenazas informáticas

Malware: Quiere decir Malicious Software, es un termino que se usa para describir a todos los software maliciosos, que tienen como objetivo infiltrarse o dañar un sistema de información sin el consentimiento del usuario.

- **Virus**: Este tipo de malware es un componente de software cuyo objetivo es permanecer en un sistema, copiándose a si mismo en varios lugares, desde el momento que se ejecuta en el sistema, así, cuando intentamos eliminar un archivo o programa infectado el virus seguirá en memoria ya que ha infectado otra parte del sistema. Su objetivo puede variar, pero en esencia es destruir o inhabilitar archivos o programas. Se replican dentro del mismo dispositivo, solo pueden infectar otros sistemas por medio de hardware, como memorias USB. Por eso se les conoce como de poca infección.

- **Gusanos:** Este malware no solo se copia a si mismo en el sistema, si no que a demás utiliza la red para copiarse a otras maquinas a través de las vulnerabilidades de la red o agujeros de seguridad. Por ello tiene una mayor capacidad de infección. El objetivo de estos gusanos es replicarse a si mismo, hasta saturar el funcionamiento del sistema.
- **Troyano:** No causan daños en si mismo, están basados en el mítico caballo de Troya, es decir, una estructura utilizada para cargar cosas ocultas, en este caso, virus, gusanos y demás malware. Los troyanos son generalmente esos programas sin licencia y cracks, que instalamos pensando que no harán ningún daño porque no somos conscientes que puede ser un Troyano. Requieren de la ejecución del usuario ya que no pueden duplicarse a si mismo. El Troyano también puede crear backdoors, que es una puerta trasera para que un dispositivo pueda ser controlado de forma remota por alguien más.
- **Adware's:** Su objetivo es bombardear nuestro dispositivo con publicidad. No son dañinos y usualmente vienen dentro de Troyanos.
- **Spywares:** o software espías, este malware no daña los dispositivos pero si roba toda la información del sistema. Su objetivo es permanecer oculto para robar todo tipo de datos, desde contraseñas, información bancaria, redes sociales, entre otros. También puede acceder por la cámara o micrófono del dispositivo sin que el usuario lo note. Suelen ingresar en Troyanos o también pueden ser instalados, como en el caso de keylogger, un spyware que registra las pulsaciones del teclado, para tener la información de lo que el usuario escribe.
- **Rootkits:** Son un conjunto de software. Los demás malware atacan al sistema operativo, entonces una vez que se reinstala el sistema, desaparece el malware. Por el contrario, los rootkits van dirigidos al firmware del sistema o los programas de usuario y tienen acceso al dispositivo en modo sistema o kernel, este acceso les permite a los rootkits realizar modificaciones a los procesos internos del sistema operativo, a los archivos del sistema como los registros e incluso a las cuentas de usuario. Logran esconderse de los softwares antimalware o antivirus.
- **Botnets:** Es la mezcla entre bot y net. Es una red de robots o un ejército de zombies que es puesto por un atacante en una red de computadoras para

ser controladas todas al mismo tiempo. Su objetivo es cometer crímenes digitales o crimeware o robo de identidad, información bancaria, chantaje, entre otros. Los Troyanos suelen ser los principales causantes de la propagación de botnets.

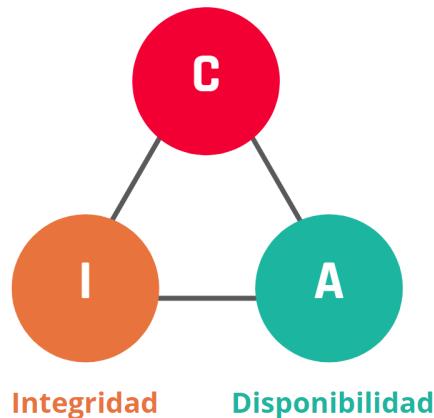
- Ransomware: o software de secuestro, suelen ser usados por atacantes contra empresas para secuestrar la información de sus servicios y productos, para luego pedir dinero a cambio de rescate. El ciber atacante hace evidente el chantaje por el secuestro y generalmente suele pedir una contraseña para poder acceder de nuevo al sistema, este tipo de malware se pueden encontrar en archivos adjuntos de correos electrónicos no deseados o al hacer click en vínculos que aseguran venir de bancos o instituciones legales, también se encuentran en redes para compartir archivos como las P2P.
 1. Ser cuidadosos con las descargas y las aplicaciones no autorizadas.
 2. Evitar páginas peligrosas.
 3. Usar un software antimalware.

Protección de la información

Información

La información es recurso clave para tomar decisiones, dimensionar cosas, y disminuir riesgos. La misma cuenta con tres dimensiones conocidas como: integridad, disponibilidad y confidencialidad, también llamadas CIA por sus siglas en inglés. Los atacantes de un sistema van a tratar de vulnerar algunas de esas dimensiones.

Confidencialidad



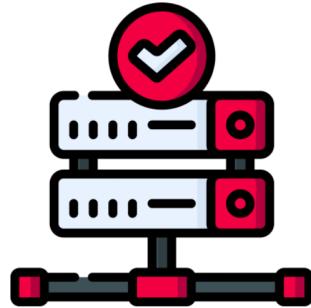
Integridad

Consiste en que la información se encuentre completa, entera y que los datos que están dentro del sistema sean los que deberían ser. Un ejemplo de esta dimensión sería el ataque a una base de datos y la modificación de los datos que hay en la misma, con lo cual podemos seguir viendo la información, pero la misma es errónea debido a que la original fue alterada.



Disponibilidad

Significa que la información una persona/usuario debe poder tener acceso a la información en el momento que lo necesita, es decir, en tiempo y forma. Un típico ataque a este tipo de dimensión es el ataque de denegación de servicio.



Confidencialidad

Refiere a que la información tiene que estar disponible únicamente para las personas que tienen acceso a esta información y bloqueada para el acceso a terceros. Por ejemplo, los datos personales e históricos médicos.



“

La **protección de la información** se basa en garantizar el completo y total funcionamiento de las 3 dimensiones, para ello, debemos implementar medidas preventivas y reactivas.



”

“

Medidas preventivas se refiere a todas las acciones que pueden tomarse para evitar problemas no deseados. Por otro lado, las **medidas reactivas** son aquellas donde ya se occasionó un problema de seguridad y hay que solventarlo.



”

Protección de la confidencialidad

La confidencialidad puede romperse de varias maneras, tanto directas (hackeando la seguridad) como indirectas a través de errores humanos. Algunas técnicas para asegurar la confiabilidad pueden ser:

| Nombre | Descripción |
|---------------------------------|---|
| Encriptación | Significa cambiar el formato de los datos con la razón de que si estos son interceptados solo las personas autorizadas sepan cómo leerlos (medida preventiva). |
| Controles de acceso | Asegurar que solo las personas autorizadas puedan acceder a la información (medida preventiva). |
| Borrado remoto | Se refiere al esfuerzo de mantener los datos siempre privados, en el caso de que se perdiera el acceso, la capacidad de bloquear el dispositivo o borrar la información (medida reactiva). |
| Capacitación al personal | Existe un concepto llamado ingeniería social , el cual es la denominación que se le da a cómo los usuarios son engañados para otorgar sus accesos, la capacitación en estos problemas es una acción preventiva para evitarlos. |

Protección de la integridad

La integridad puede romperse de varias maneras similares a la de la confiabilidad, por lo cual, varias de sus acciones de seguridad son reutilizadas. Algunas técnicas para asegurar la integridad pueden ser:

| Nombre | Descripción |
|--------------------------------|---|
| Auditorias | Se utilizan para comprobar que la información coincide con lo que debería ser correcto (medida reactiva). |
| El control de versiones | Si ha ocurrido un inconveniente con la información, diversas herramientas de control de versiones ayudan a "volver a un estado anterior" (medida reactiva). |
| Firmas digitales | Esta medida permite asegurar la autenticidad del documento (medida preventiva). |
| Detección de intrusos | Diseñados para detectar problemas cuando un acceso no autorizado se ha cometido (medida reactiva). |

Protección de la disponibilidad

La disponibilidad debe tenerse en cuenta para cuando ocurra un problema de seguridad como de forma preventiva al mismo. Algunas técnicas para asegurar la disponibilidad pueden ser:

| Nombre | Descripción |
|----------------------|---|
| Tolerancia a fallos | La capacidad de los sistemas o servidores a que si algún tipo de fallo sucede, la información pueda ser utilizada (preventiva o reactiva dependiendo la situación). |
| Redundancia | De esta forma la información y las validaciones de acceso se repitan tanto que la información está segura de no perderse en su totalidad (preventiva). |
| Parches de seguridad | Cuando se detecta una falla, debe solucionarse el problema para que no vuelva a ocurrir, igualmente si la falla fue por un software, actualizarlo con la vulnerabilidad resuelta. |

Fallas y vulnerabilidades

“

Una **falla**, también conocida como bug, es un **error** en un programa o sistema operativo que desencadena un resultado indeseado.



”

“

El término **bug** viene desde 1947 cuando Grace Hopper, mientras estaba programando el Mark II, descubrió que un **insecto** (bug) había provocado un error en uno de sus relés electromagnéticos.



”

“

En el desarrollo del software existen muchos tipos de fallas, pero en general se pudieron establecer unos tipos generales de bugs según su comportamiento.



”

Tipos de fallas

| Nombre | Descripción |
|------------------------|---|
| Heisenbug | Basados en el principio de incertidumbre de Heisenberg se denominan a aquellos bugs que alteran o desaparecen su comportamiento al tratar de depurarlos. |
| Bohrbug | Nombrados así por el modelo atómico de Bohr, es una clasificación de un error de software inusual que siempre produce una falla al reiniciar la operación que causó la falla. |
| Mandelbug | Llamado así por el matemático Benoit Mandelbrot, un mandelbug es un fallo con causas tan complejas que su comportamiento es totalmente caótico. |
| Schroedelinbugs | Son errores que no aparecen hasta que alguien lee el código y descubre que, en determinadas circunstancias, el programa podría fallar. A partir de ese momento, el "Schroedelinbug" comienza aparecer una y otra vez. |

“

Una **vulnerabilidad** es una debilidad o fallo de un sistema informático que puede poner en riesgo la integridad, confidencialidad o disponibilidad de la información.



”

“

La evaluación o detección de vulnerabilidades permite reconocer, clasificar y caracterizar los agujeros de seguridad.



”

Pasos para detectar una vulnerabilidad

Si bien no existe un método único para detectar vulnerabilidades, es posible armar una serie de ítems a tener en cuenta para considerar nuestra información segura.

- Evaluar cómo está constituida la red e infraestructura de la empresa.
- Delimitar quién puede y debe acceder a la información confidencial.
- Probar que las copias de seguridad realizadas funcionen.
- Identificar las partes más sensibles y esenciales del sistema.
- Realizar auditorías del estado de la seguridad informática.